

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-269959

(43)Date of publication of application : 29.09.2000

(51)Int.Cl. H04L 9/32

H04Q 7/38

H04L 9/08

(21)Application number : 11-317628

(71)Applicant : LUCENT TECHNOLOG INC

(22)Date of filing : 09.11.1999

(72)Inventor : BERENZWEIG ADAM L
BRATHWAITE CARLOS
ENRIQUE

(30)Priority

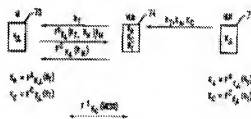
Priority number : 98 188818 Priority date : 09.11.1998 Priority country : US

(54) AUTHENTICATION METHOD BY UPDATED KEY

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain an efficient authentication execution method that uses an authentication call sent to a terminal so as to supply information about the authentication, and to calculate an encryption key to the terminal.

SOLUTION: A visiting authentication center obtains a random number RT, an authentication key KA, and an encryption key KC from a host authentication center. The visiting authentication center transmits a random number RT to a transmitter to update an authentication key and an encryption key of the terminal and calls the terminal as a part of an authentication process. The terminal calculates the authentication key KA and the encryption key KC by using the RT and replies the call from the visiting authentication center. In addition, a reply of a visiting network to the authentication call of the terminal to the network is checked by using the authentication key.



(51) Int.Cl. ⁷	識別番号	F I	キーワード (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
			6 7 5 B
審査請求 未請求 請求項の数20 ○ L (全 7 頁)			
(21) 出願番号	特願平11-317628	(71) 出願人	596092698 ルーセント テクノロジーズ インコーポ レーテッド アメリカ合衆国, 07974-0636 ニュージ ヤージー, マレイ ヒル, マウンテン ア ヴェニュー 600
(22) 出願日	平成11年11月9日 (1999. 11. 9)	(72) 発明者	アダム エル. プレンズウエイグ アメリカ合衆国 10003 ニューヨーク, ニューヨーク, ナンバー12-0, イースト ツェルヴス ストリート 70
(31) 優先権主張番号	0 9 / 1 8 8 8 1 8	(74) 代理人	100064447 弁理士 岡部 正夫 (外11名)
(32) 優先日	平成10年11月9日 (1998. 11. 9)		
(33) 優先権主張国	米国 (U S)		

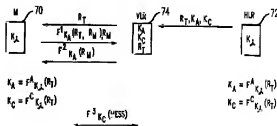
最終頁に続く

(54) 【発明の名称】 キー更新による認証方法

(57) 【要約】

【課題】 本発明は、端末装置に伝送された認証呼掛けを用い、認証と暗号キー値を計算するための情報を端末装置に供給する、効率的な認証実行方法を提供することを目的とする。

【解決手段】 ビジティング認証センタはホーム認証センタより、ランダム値R T、認証キー値K A、および暗号キー値K Cを得る。ビジティング認証センタはランダムナンバーR Tを端末装置に伝送し、端末装置の認証キーと暗号キー値とを更新し、また、認証プロセスの部分として端末装置に呼掛けする。端末装置はR Tを用いて認証キー値K Aおよび暗号キー値K Cを計算し、かつ、ビジティング認証センタの呼掛けに応答する。加え、認証キー値を用いて、ネットワークへの端末装置の認証呼掛けに対するビジティングネットワークの応答を検査する。



【特許請求の範囲】

【請求項1】 認証方法において、
第一の値を端末装置に伝送するステップと、
第一の応答値が、入力として第一の値の少なくとも第一の部分およびキー入力として第一のキー値とを用いる第一の暗号関数の少なくとも出力の部分であり、第一のキー値が、入力として第一の値の少なくとも第二の部分およびキー入力として第二のキー値とを用いる第二の暗号関数の出力の少なくとも一部分であって、少なくとも第一の応答値を有する端末装置からの応答を受信するステップと、第一の応答値が予測された第一の応答値と等しいことを検査するステップとからなる認証方法。

【請求項2】 請求項1に記載の方法において、第二のキー値は端末装置と関連することを特徴とする方法。

【請求項3】 請求項1に記載の方法において、第一の暗号関数および第二の暗号関数は同一であることを特徴とする方法。

【請求項4】 請求項1に記載の方法において、第一の部分と第二の部分とは同一であることを特徴とする方法。

【請求項5】 請求項1に記載の方法において、応答が第二の応答値を有し、第二の値を端末装置に伝送するステップをさらに有し、第二の値は入力として第二の応答値の少なくとも一部分とキー入力として第三のキー値とを用いる、第三の暗号関数の出力の少なくとも一部分であることを特徴とする方法。

【請求項6】 認証方法において、
第一の値を端末装置に伝送するステップと、
第一の応答値が、入力として第一の値の少なくとも第一の部分と第二の応答値の少なくとも第一の部分とキー入力として第一のキー値とを用いる第一の暗号関数の少なくとも出力の部分であり、第一のキー値が、入力として第一の値の少なくとも第二の部分およびキー入力として第二のキー値とを用いる第二の暗号関数の出力の少なくとも一部分であって、少なくとも第一の応答値と第二の応答値とを有する端末装置からの応答を受信するステップと、
第一の応答値が予測された第一の応答値と等しいことを検査するステップとからなる認証方法。

【請求項7】 請求項6に記載の方法において、第二のキー値は端末装置と関連することを特徴とする方法。

【請求項8】 請求項6に記載の方法において、第一の暗号関数および第二の暗号関数は同一であることを特徴とする方法。

【請求項9】 請求項6に記載の方法において、第一の値の第一の部分と第二の部分は同一であることを特徴とする方法。

【請求項10】 請求項6に記載の方法において、第二の値を端末装置に伝送するステップを有し、第二の値は入力として第二の応答値の少なくとも第三の部分とキー入力として第三のキー値とを用いる第三の暗号関数の出

力の少なくとも一部分であることを特徴とする方法。

【請求項11】 認証方法において、
第一の値を受信するステップと、
第一の応答値が、入力として第一の値の少なくとも第一の部分とキー入力として第一のキー値とを用いる第一の暗号関数の少なくとも出力の部分であり、第一のキー値が、入力として第一の値の少なくとも第二の部分とキー入力として第二のキー値とを用いる第二の暗号関数の出力の少なくとも一部分であって、少なくとも第一の応答値を有する応答を伝送するステップとからなる認証方法。

【請求項12】 請求項11に記載の方法において、第一の暗号関数および第二の暗号関数は同一であることを特徴とする方法。

【請求項13】 請求項11に記載の方法において、第一の部分と第二の部分は同一であることを特徴とする方法。

【請求項14】 請求項11に記載の方法において、応答は第二の応答値を有し、第二の値を受信するステップをさらに含み、第二の値は、入力として第二の応答値の少なくとも一部分とキー入力として第三のキー値とを用いる第三の暗号関数の出力の少なくとも一部分であることを特徴とする方法。

【請求項15】 請求項14に記載の方法において、第二の値が予測された第二の値と等しいことを検査するステップをさらに含む方法。

【請求項16】 認証方法において、
第一の値を受信するステップと、
第一の応答値が、入力として第一の値の少なくとも第一の部分と第二の応答値の少なくとも第一の部分とキー入力として第一のキー値とを用いる第一の暗号関数の少なくとも出力の部分であり、第一のキー値が、入力として第一の値の少なくとも第二の部分とキー入力として第二のキー値とを用いる第二暗号関数の出力の少なくとも一部分であって、少なくとも第一の応答値と第二の応答値とを有する応答を伝送するステップとからなる認証方法。

【請求項17】 請求項16に記載の方法において、第一の暗号関数および第二の暗号関数は同一であることを特徴とする方法。

【請求項18】 請求項16に記載の方法において、第一の値の第一の部分と第二の部分は同一であることを特徴とする方法。

【請求項19】 請求項16に記載の方法において、第二の値を受信するステップをさらに含み、第二の値は、入力として第二の応答値の少なくとも一部分とキー入力として第三のキー値とを用いる第三の暗号関数の出力の少なくとも一部分であることを特徴とする方法。

【請求項20】 請求項19に記載の方法において、第二の値が予測された第二の値と等しいことを検査するステップを有することを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は通信に関するものであり、さらに詳しく言うと、無線通信システムにおける通信者の認証に関するものである。

【0002】

【従来技術】図1は、基地局10と、これに関連するセル12と、セル12内にあるモバイル14とを示している。最初に、モバイル14が基地局10との通信をレジスタするか、又は通信を試みる場合、モバイルの通信ネットワークへのアクセスが許可される前に、基地局10がモバイル識別検査、認証を行う。モバイル14がそのホームネットワーク以外のネットワーク内にある場合、

ビジティングネットワーク内にあるとして認証が行われる。ホームネットワークとは、モバイル端末所有者と契約を交し、無線通信サービスを提供するサブスクリバによって制御がなされるネットワークのことをいう。モバイルがビジティング通信ネットワークで作動する場合、基地局10がモバイルを認証する際、モバイルのホームネットワークの認証センタ16との通信が必要となる。図1の例においては、モバイル14はビジティングネットワーク内にある。結果、モバイル14の認証にはモバイルのホームネットワークの認証センタ16との通信を必要とする。モバイル14がビジターネットワークにアクセスを試みると、基地局10はビジティング通信ネットワークの認証センタ18との通信を行う。認証センタ18は、モバイル14の電話番号といったようなモバイルや端末の識別子によって、モバイル14がホーム認証センタ16を使用するネットワークにレジスタされていることを判断する。次に、ビジティング認証センタ18はIS41番号ネットワーク20のようなネットワーク上でホーム認証センタ16と通信を交す。次に、ホーム認証センタ16は、モバイル14の登録エントリーを有するホーム位置レジスタ22にアクセスする。ホーム位置レジスタ22は、モバイルの電話番号といったような識別子によって端末もしくはモバイルと連動する。ホーム位置レジスタに蓄積された情報は、暗号キー発行や、ビジタ認証センタのビジタ位置レジスタ24に供給される他の情報の発信に使用される。次に、ビジタ位置レジスタ24からの情報は、モバイル14に伝送される情報を基地局10に供給することになる。これにより、モバイル14は応答可能となり、かつ、それにより通信サービスを受ける資格を有したモバイルであるとの認証がなされる。

【0003】図2は、GSM無線ネットワークで使用される認証工程図である。この場合、モバイルとホーム位置レジスタの両方はキー-K1を有する。モバイルがビジティングネットワークへのアクセスをリクエストすると、ビジティング認証センタはホーム認証センタにコンタクトし、変数RAND、SRES、およびKcを受取

る。ホーム認証センタはモバイルと関連するホーム位置レジスタからの値Kiを使用し、値SRES、および値Kcを発する。値SRESは、入力としてランダムナンバRAND、かつ、キー入力として値Kiとにより、A3として知られる暗号関数を用いて計算される。同様の方法で、暗号キーKcは、入力としてRAND、かつ、キー入力として値Kiとにより、暗号関数A8を用いて計算される。これらの値はビジティング認証センタのビジタ位置レジスタに転送される。次に、ビジティング認証センタはモバイルにランダムナンバRANDを伝送することにより、モバイルに呼び出す。モバイルは、ホーム認証センタによって行われた計算方法と同方法でSRES、およびKcを計算する。次にモバイルは、値SRESをビジティング認証センタに伝送し、そこでビジティング認証センタはモバイルより受信のSRESとホーム認証センタから受信のSRESとを比較する。これらの値がマッチした場合、モバイルのビジティングネットワークへのアクセスが許可となる。モバイルと、ビジティングネットワーク間の通信がさらに暗号化される場合、入力として暗号化されるメッセージと、かつ、値Kcと等しいキー入力とにより、A5暗号関数を用いることにより、これらが暗号化される。暗号関数A3、A5、およびA8は従来技術でよく知られており、GSM標準により推奨されている。GSMシステムにおいて、ホーム認証センタとの通信を含むこの認証プロセスは、モバイルがビジティングネットワークで新規コールを開始する毎に実行される。

【0004】図3aおよび図3bは、IS41コンプライアントネットワークに使用される認証プロセス図である。IS41コンプライアントネットワーク例は、AMPS（アドバンスドモバイルサービス）、TDMA（時分割多元接続）、もしくはCDMA（コード分割多元接続）プロトコルを用いるネットワークである。このシステムにおいて、モバイルとホーム位置レジスタの両方はKEYとと呼ばれるシークレット値を含んでいる。モバイルがビジティングネットワークへのアクセスをリクエストすると、ビジティングネットワーク認証センタはホーム認証センタからのデータをリクエストする。実際の認証プロセス開始前に、モバイルとビジタ位置レジスタとの両方に認証および通信のための暗号アルゴリズムにて使用されるキーを供給することによりキー更新が実行される。モバイルと関連するホーム位置レジスタは、モバイルの電話番号といったような識別子を用い所在場所が確認され、また、ホーム位置レジスタに保存されたKEY値は、ビジタ位置レジスタへの伝送データを作り出すことに使われる。計算された値は、SSDA（共用シークレットデータA）値とSSDB（共用シークレットデータB）値である。これらの値は、入力としてランダムナンバrsと、キー入力として値KEYとを用い、CAVEアルゴリズムを実行することにより

計算される。CAVEアルゴリズムは、従来技術でよく知られており、IS41スタンダードに詳述されている。ホーム認証センタは値R_s、SSDA、およびSSDBを、ビジティングネットワークのビジター位置レジスタに転送する。これをうけて、ビジティングネットワークは、R_sをモバイルに伝送することにより、モバイルで使用することになる共用シークレットデータ(SSDAおよびSSDB)を更新する。次に、モバイルは、ホーム認証センタにより行われた方法と同計算方法でSSDAおよびSSDBを計算する。ここでモバイルとビジター位置レジスタの両方がSSDA値およびSSDB値を有することで認証プロセスが開始される。

【0005】図3bは、モバイルとビジター位置レジスタとの両方がキーSSDAおよびSSDBを受取った後、いかにモバイルがビジティングネットワーク内で認証されるかを示したものである。ビジティング認証センタは、ランダムナンバR_Nをモバイルに送信することによりモバイルに呼掛けを行う。この時点で、モバイルとビジティング認証センタの両方は値AUTHRを計算する。AUTHRは、入力としてランダムナンバR_Nと、キー入力としてSSDA値を用いるCAVEアルゴリズムの出力と等しい。次にモバイルは計算された値AUTHRをビジティング認証センタに伝送する。ビジティング認証センタはそのAUTHRの計算値と、モバイルから受けた値との比較を行う。値がマッチした場合、モバイルは認証され、ビジティングネットワークへのアクセスが可能となる。加え、モバイルとビジティング認証センタの両方は、暗号キーK_cの値を計算する。この時点で、モバイルとビジティングネットワーク間の通信が許可され、暗号関数を用いて暗号化されるであろう。そこで、入力は暗号化されるメッセージと、キーK_cである。暗号関数はそれぞれの標準によってCDMAシステムおよびTDMAシステムが指定される。IS41に関して、ビジティング認証センタとホーム認証センタ間の通信は、モバイルに呼出される度ではなく、モバイルがビジティングネットワークにレジスタする度に毎にのみ行われることを注記する。

【0006】上述の方法は、モバイルがネットワークにアクセスする許可を得るためのその検査方法を示したものである。しかし、上記の方法では正規ネットワークによりそれ自身を確認することが問われるモバイル検査については論じていない。図4は、ビジティングネットワークとモバイル間の相互認証を可能にするIS41スタンダードの改善案である。図4は、図3aに関して上記で論じたように、一旦、モバイルとビジター位置レジスタの両方が値SSDAおよび値SSDBを受取った時の相互認証プロセスを図示したものである。ビジティングネットワークはランダムナンバR_Nを伝送することによ

りモバイルに呼掛けを行う。次に、モバイルは計算実行により応答し、入力として値R_NおよびR_Mと、キー入力として値SSDAとを用い、暗号関数F1の出力を得る。この場合、R_Nはビジティングネットワークにより伝送された値と同値であり、R_Mはモバイルにより計算が行われたランダムナンバである。暗号関数の出力伝送に加え、値R_Mもまた非暗号化フォームでビジティングネットワークに伝送される。ビジティングネットワークは、キー入力として値SSDAにより、F1暗号関数への入力としてR_Mの非暗号化フォームと値R_Nとを用いて、F1暗号関数の出力を計算する。この出力値は、モバイルから受取った値と比較され、これらがマッチした場合、モバイルが検査、認証される。次に、ビジティングネットワークは、値R_Mのフォームでモバイルより供給された呼掛けに応答することによって、モバイルにより認証、検査される。ビジティング認証センタは、入力として値R_Mと、キー入力として値SSDAとを用いて、暗号関数F2の出力を伝送する。次に、モバイルは同様の計算を行い、キーSSDAおよび値R_Mとを用いて、ビジティングネットワークから受取った値と、暗号関数F2の出力から得た値とを比較する。これらの値がマッチした場合、モバイルは認証、検査されたネットワークを考え、そのネットワークとの通信を継続する。ビジティング認証センタとモバイルの両方は、入力として値R_NおよびR_Mと、キー入力として値SSDBとを用いて、暗号関数F3の出力を得ることにより、暗号キーK_cの値を計算する。この時点で、モバイルとビジティングネットワークとが通信可能となる。この時、万一、暗号通信が所望される場合、入力として暗号化されるメッセージと、キー入力として値K_cとにより、暗号アルゴリズムF4を用い、メッセージが暗号化される。暗号関数F1、F2、およびF3は、ハッシュ関数であるか、又はSHA-1等の1つの暗号関数であり、関数F4はDESであるような暗号関数であろう。ハッシュ関数や、SHA-1といったような一方向性暗号関数や、DESといったような暗号関数は従来技術においてよく知られている。

【0007】

【発明が解決しようとする課題】しかしながら、上述の従来の相互認証プロセスにおいては、認証プロセスを開始する前に、モバイルとビジター位置レジスタとの両方が値SSDAおよび値SSDBとを有することが必要であることから、その非効率さに悩まされている。結果、モバイルとビジティング認証センタ間に少なくとも2セットの通信が必要となる。通信の第一セットにおいては、値SSDAおよび値SSDBの計算に使用される情報をモバイルに供給する。通信の第二セットでは、相互認証の実行に使用される。

【0008】

【課題を解決するための手段】本発明は、認証及び暗号

割賦キーの値を計算するために端末装置に情報を提供するように、端末装置に伝送される認証呼かけを使用することによって、認証を実行するためのより効果的な方法を提供する。結果、端末装置にキー値を供給するための別々の通信を必要とせず、非効率的なセット通信を解消する。ビジティング認証センタはホーム認証センタより、ランダム値R T、認証キー値K A、および暗号キー値K Cを得る。ビジティング認証センタはランダムナンバーTを端末装置に伝送し、端末装置の認証キーと暗号キー値とを更新し、また、認証プロセスの部分として端末装置に呼掛けする。端末装置はR Tを用いて認証キー値K Aおよび暗号キー値K Cを計算し、かつ、ビジティング認証センタの呼掛けに応答する。加え、認証キー値を用いて、ネットワークへの端末装置の認証呼掛けに対するビジティングネットワークの応答を検査する。

【0009】

【発明の実施の形態】図4は、モバイルもしくは固定端末に伝送されたシングルランダム値を用いて、端末装置の認証および暗号キー値を更新し、さらに、端末装置への認証呼かけを行う方法を図示したものである。モバイルもしくは固定端末7 0、およびホーム位置レジスタ7 2は認証キー値K iを共有する。モバイル端末7 0がビジティングネットワークへのアクセスリクエストを行うと、ビジティング認証センタはホーム認証センタにコンタクトし、ランダム値R T、認証キー値K A、および暗号キー値K Cとを得る。このリクエストに応え、ホーム認証センタは、ビジティング認証センタ経由でモバイル端末より提供された電話番号等の識別子を用い、モバイル端末7 0と関連するホーム位置レジスタ7 2にアクセスする。次に、ホーム認証センタは、入力としてランダムナンバーTと、キー入力として値K iとを用いて、暗号関数F Aの出力を得ることにより認証キー値K Aを計算する。加え、ホーム認証センタは、入力として値R Tを、またキー入力として値K iとを用い、暗号関数F Cの出力を用いて暗号キー値K Cを計算する。一旦、これらの計算が行われると、ホーム認証センタは値R T、K A、およびK Cをビジティング認証センタに通信する。ビジティング認証センタは、モバイル端末7 0と関連するビジター位置レジスタに値K A、K CおよびR Tを保存する。次に、認証呼かけとして、かつ、モバイル端末で使われた暗号キー値および認証を更新するために使用する値として、ビジティング認証センタは値R Tをモバイル端末7 0に通信する。モバイル端末はビジティング認証センタより受取った値R Tを用い、ホーム認証センタで行った計算方法と同様の方法で、認証キー値K Aおよび暗号キー値K Cとを計算する。次に、モバイル端末は認証キー値K Aを用い、ビジティング認証センタの認証呼かけに応答する。モバイル端末は入力として値R TおよびR Mと、かつ、キー入力として認証キー値K Aとを用いて、暗号関数F 1の出力を判断する。しかし、入力

として、R TおよびR Mの両方でなく、値R Tを用いることも可能である。暗号関数F 1および値R Mの出力はビジティング認証センタに通信される。しかし、R Mが暗号関数F 1の入力として使用されなかった場合や、ネットワークの認証が必要とされない場合は、値R Mの伝送は行われない。値R Mはモバイル端末より選択されたランダム値である。ビジティング認証センタは入力R TおよびR M、およびキー入力値K Aにより関数F 1の出力値を計算する。それにより、モバイル端末より通信された値とその結果とが比較可能となる。値がマッチした場合、モバイル端末はビジティングネットワークにより、照合又は認証される。モバイル端末より供給された値R Mは、モバイル7 0によるビジティングネットワークへの認証呼掛けに用いられる。ビジティングネットワークは、入力として値R Mを、また、キー入力として値K Aとを用い関数F 2の出力を計算する。この出力値はモバイル端末に通信される。モバイル端末は、入力として値R Mを、かつ、キー入力として値K Aとより関数F 2の出力を別個に判断し、これらの出力値がマッチした場合に、モバイル端末はビジティングネットワークの照合又は認証する。モバイル端末とビジティングネットワークの両方が互いに識別検査、認証を一旦行うと、通信は継続する。通信は非暗号化メッセージもしくは暗号化メッセージを用いることにより交わされる。暗号化メッセージが使用される場合、入力としてメッセージを、かつ、キー入力として暗号値K Cとにより、暗号関数F 2の出力を用いてメッセージが暗号化される。このプロセスは、モバイル端末とビジティングネットワーク間においてコールが試みられる度毎に実行される。もしくは、コールが試みられるその度毎ではなく、モバイルがビジティングネットワークにレジスタする度毎にホーム認証センタにコンタクトすることも可能である。また、モバイルがビジティングネットワークにレジスタされたままであるかぎり、K A、K C、およびR Tの同一値を使用することも可能である。暗号関数F 1、F 2、F A、およびF Cはハッシュ関数であるか、もしくはS H A-1のような1暗号関数であろう。また、関数F 3はD E Sのような暗号関数であろう。ハッシュ関数、S H A-1のような一方性暗号関数、およびD E Sのような暗号関数は従来技術によってよく知られている。

【0010】モバイル端末がホームネットワーク内にある場合にも、同工程の実行が可能である。この場合、ビジティング認証センタではなく、ホーム認証センタがモバイル端末と通信を行う。無線通信において、端末と認証センタ間の通信は無線基地局を通過して行われる。

【図面の簡単な説明】

【図1】モバイル、ビジティングネットワーク、およびホームネットワーク間の通信を図示したものである。

【図2】G S Mネットワークの認証プロセス図である。

【図3 a】I S 4 1コンプライアントネットワークのキ

一更新および認証プロセスを图示したものである。

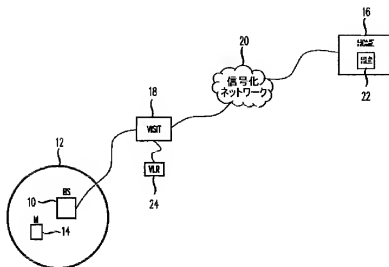
【図3b】 I S 4 1 コンプライアントネットワークのキー更新および認証プロセスを图示したものである。

【図4】 従来技術による相互認証方法を图示したもので

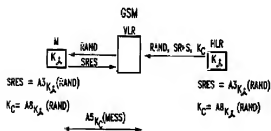
ある。

【図5】 本発明によるキー更新および相互認証の実行方法である。

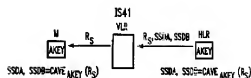
【図1】



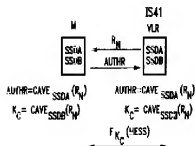
【図2】



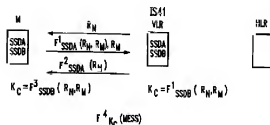
【図3a】



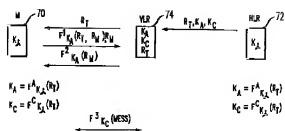
【図3b】



【図4】



【図5】



フロントページの続き

(72)発明者 カルロス エンリキエー ブラスウェイト
 アメリカ合衆国 07050 ニュージーヤシ
 イ, オレンジ, ヒルヤー ストリート 63